STATE OF TENNESSEE
DIVISION OF MENTAL RETARDATION SERVICES
HIPAA POLICY - Privacy

POLICY TITLE: General Privacy

Policy Number: DMRS HIPAA 102 **Effective Date: January 1, 2004**
Deputy Commissioner:

I. PURPOSE

This policy will provide guidelines for all employees of the Division of Mental Retardation Services (DMRS) regarding the security and privacy of protected health information. It will assure that the health information of all service recipients will remain confidential and that reasonable efforts will be made to safeguard this information.

II. SCOPE

The policy will apply to all protected health information created or received at DMRS agencies, including medical records, shadow records, billing records, health plan records, and electronic records. It will also apply to indexes, logs, ledgers, and reports containing protected health information.

III. AUTHORITY

Department of Health and Human Services Standards for Privacy of Individually Identifiable Health Information, Final Rule, 45 CFR Parts 160 and 164: Title 33 of the *Tennessee Code Annotated.*

IV. POLICY

DMRS will take every precaution to make sure service recipients' protected health information is transmitted and maintained in the most secure and private manner.
Definitions:
Health Care Operations: Activities related to quality assessment and improvement, the competence or qualifications of health care professionals, health insurance benefits, medical review, legal services, auditing functions, business planning and development, business management and general administrative activities

Health Information: Information whether oral or recorded in any form or medium that is created or received and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or past, present or future payment for the provision of health care to an individual

Individually Identifiable Health Information: Health information that identifies an individual or that can be used to identify an individual

Payment: Activities undertaken in order to obtain reimbursement, including determinations of eligibility or coverage, billing and claims management, medical necessity, utilization review and collections

Protected Health Information (PHI) means individually identifiable information relating to past, present or future physical or mental health or condition of an individual, provision of

health care to an individual, or the past, present or future payment for health care provided to an individual.

Shadow Record: A record maintained by an individual or department which is a duplication of original documents maintained elsewhere

Treatment: The provision, coordination, or management of health care and related services, including consultations and referrals

Workforce Members means employees, volunteers, trainees, contractors, and other persons whose conduct, in the performance of work for the department, its offices, or programs onsite under the direct control of the department, office, or program regardless of whether they are paid by the Division of Mental Retardation Services.

POLICY OVERVIEW

A privacy officer is to be appointed for DMRS, each regional office, and each developmental center. The privacy officer will be responsible for the development and implementation of policies and procedures of the respective entity. This individual will also be a resource for the workforce and will be available to answer questions and address issues regarding the privacy and security of health information.

A. A contact person or office will be designated for DMRS, each regional office, and each developmental center for the purpose of receiving complaints regarding HIPAA and for providing further information as necessary. Complaints will be addressed in a timely manner and documented by each agency.

B. All appropriate members of the workforce will be trained initially on policies and procedures regarding protected health information as necessary for them to carry out their function within the entity. Each new employee will be trained within 30 days after joining or rejoining the workforce, and all members of the workforce will be re-trained following significant revisions to policies and procedures. Documentation of all training will be maintained.

C. Appropriate sanctions, including civil penalties and disciplinary action up to and including termination, will be taken against members of the workforce who fail to comply with privacy practices. The consequences on non-compliance will be communicated to the workforce during initial training. All sanctions will be documented.

D. DMRS, each regional office, and each developmental center must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

E. Access to protected health information by DMRS employees will be limited to the minimum necessary amount of information that is required in order for them to optimally carry out their job responsibilities. Classes of employees who need access to protected health information will be identified by each agency and this information will be communicated to each employee by the supervisor initially upon hire and thereafter at the time of the job planning discussion. It is the

responsibility of each employee to be aware of these designations and to abide by them.

F. DMRS must attempt to mitigate any harmful effect that occurs as a result of violation of polices and procedures regarding protected health information.

G. DMRS will refrain from intimidating or retaliatory acts toward individuals and others who have filed a complaint regarding privacy practices, participate in any proceeding, or oppose a privacy practice. DMRS will not require an individual to waive their rights as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility of benefits.

H. Policies and procedures will be revised to comply with changes in law and and DMRS will maintain these polices and procedures in written or electronic form for six years.

V. IMPLEMENTATION

A. A Confidentiality Statement is to be signed by each member of the workforce upon employment. Each work site will be responsible for maintaining these statements and providing documentation.

B. A Notice of Privacy Practices will be mailed initially to each service recipient and thereafter when there is a significant change to the notice. The notice will be posted on the DMRS web site and should be posted in each work site which has a direct care relationship with an individual. An attempt to obtain an acknowledgment form of receipt should be made by those agencies having a direct care relationship with an individual. Any change in the notice will be communicated to service recipients.

C. Protected health information from any source must not be left unattended. Offices, file cabinets, desks, and storage areas should be locked when staff are not present and care must be taken not to leave protected health information in public areas.

D. Protected health information maintained on electronic media will be properly labeled, stored, and safeguarded.

E. Screen savers, passwords, and unique IDs for computer system access will be maintained.

F. Fax machines and printers used for protected health information must be secure and inaccessible to unauthorized persons. Each agency will be responsible for developing procedures that protect the security of this information.

G. Computer monitors should be positioned so that unauthorized persons do not have access to protected health information.

H. Mail shared within DMRS and its agencies should be placed in interdepartmental envelopes and stored in secure areas. As an extra security measure protected health information may be marked confidential on the outside of the transmission.

I. Protected health information no longer needed is to be destroyed. Each work site will be responsible for determining means of destruction in accordance with State approved methods for protected health information and assuring that employees are in compliance. Each work site will also be responsible for assuring that information stored prior to destruction is protected from unauthorized access.

J. Employees will take reasonable precautions to avoid incidental disclosure of protected health information whether written, electronic, or oral. Such disclosures will be allowed as necessary for employees to carry out their job responsibilities. Incidental disclosures will not result in sanctions but employees will be encouraged to minimize this occurrence.

K. Reports will be reviewed on a regular basis to determine the necessity of the report, whether it contains protected health information, and to assure that it is limited to the minimum necessary information and is distributed only to staff who have a need to know the information as part of their job responsibilities.

L. Protected health information, whether written, electronic, or oral, is not to leave the work site without approval of the immediate supervisor or privacy officer, or by court order or subpoena.

M. Violations of privacy will be reviewed by the privacy officer and the privacy committee, if applicable, and recommendations regarding sanctions will be made.